PCT/JP00/03838

EV

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

14.06.00
04 AUG 2000

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　５月２３日

出願番号
Application Number: 特願２０００－１５１８７９

出願人
Applicant (s): 株式会社エヌ・ティ・ティ・ドコモ

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２０００年　７月２１日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０５７５５２

【書類名】　特許願
【整理番号】　DCMH110358
【提出日】　平成12年 5月23日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L 9/00
【発明の名称】　通信システム、通信方法および通信ユニット
【請求項の数】　9
【発明者】
【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
【氏名】　福本　雅朗
【発明者】
【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
【氏名】　杉村　利明
【特許出願人】
【識別番号】　392026693
【氏名又は名称】　株式会社エヌ・ティ・ティ・ドコモ
【代理人】
【識別番号】　100098084
【弁理士】
【氏名又は名称】　川▲崎▼　研二
【選任した代理人】
【識別番号】　100111763
【弁理士】
【氏名又は名称】　松本　隆
【選任した代理人】
【識別番号】　100108936
【弁理士】

【氏名又は名称】　秦　貴清

【手数料の表示】

【予納台帳番号】　038265

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信システム、通信方法および通信ユニット

【特許請求の範囲】

【請求項１】　通信端末と、サーバとを具備し、

前記通信端末は、第１および第２の端末側通信手段を具備し、

前記サーバは、第１および第２のサーバ側通信手段を具備し、

前記通信端末の第１の端末側通信手段と前記サーバの第１のサーバ側通信手段は、インターネットを含まない１または複数の通信網を介して、秘匿を必要とする情報の通信を行い、

前記通信端末の第２の端末側通信手段と前記サーバの第２のサーバ側通信手段は、インターネットを含む１または複数の通信網を介して、秘匿を必要としない情報の通信を行う

ことを特徴とする通信システム。

【請求項２】　通信端末と、サーバとを具備し、

前記通信端末は、第１および第２の端末側通信手段を具備し、

前記サーバは、第１および第２のサーバ側通信手段を具備し、

前記通信端末の第１の端末側通信手段と前記サーバの第１のサーバ側通信手段は、インターネットを含まない１または複数の通信網を介して、セッション鍵の交換を行い、

前記通信端末の第２の端末側通信手段と前記サーバの第２のサーバ側通信手段は、インターネットを含む１または複数の通信網を介して、前記セッション鍵によって暗号化された情報の通信を行う

ことを特徴とする通信システム。

【請求項３】　通信端末が、第１の通信手段により、インターネットを含まない１または複数の通信網を介して、前記サーバとの間で、秘匿を必要とする情報の通信を行う過程と、

前記通信端末が、前記第１の通信手段とは別の第２の通信手段により、インターネットを含む１または複数の通信網を介して、前記サーバとの間で、秘匿を必要としない情報の通信を行う過程と、を具備する

ことを特徴とする通信方法。

【請求項４】　通信端末が、第１の通信手段により、インターネットを含まない１または複数の通信網を介して、サーバとの間で、セッション鍵の交換を行う過程と、

前記通信端末が、前記第１の通信手段とは別の第２の通信手段により、インターネットを含む１または複数の通信網を介して、前記サーバとの間で、前記セッション鍵によって暗号化された情報の通信を行う過程と、を具備する

ことを特徴とする通信方法。

【請求項５】　通信端末が、第１の通信手段により、インターネットを含む１または複数の通信網を介して、電子ショップサーバとの間で、商品の購買を行い、購入した商品を指定した購買タグを受信する過程と、

前記通信端末が、前記第１の通信手段とは別の第２の通信手段により、インターネットを含まない１または複数の通信網を介して、前記電子ショップサーバとの間で、前記購買タグおよび秘匿を必要とする個人情報の通信を行う過程と、

前記電子ショップサーバが、前記購買タグおよび個人情報を用いて決済を行う過程と、を具備する

ことを特徴とする通信方法。

【請求項６】　通信端末が、第１の通信手段により、インターネットを含まない１または複数の通信網を介して、電子ショップサーバとの間で、セッション鍵の交換を行う過程と、

前記通信端末が、前記第１の通信手段とは別の第２の通信手段により、インターネットを含む１または複数の通信網を介して、前記電子ショップサーバとの間で、前記セッション鍵によって暗号化された情報で商品の購買を行い、購入した商品を指定した購買タグを記憶する過程と、

前記通信端末が、前記第１の通信手段により、インターネットを含まない１または複数の通信網を介して、前記電子ショップサーバとの間で、前記購買タグおよび秘匿を必要とする個人情報の通信を行う過程と、

前記電子ショップサーバが、前記購買タグおよび個人情報を用いて決済を行う過程と、を具備する

ことを特徴とする通信方法。

【請求項７】　外部ユニットに装着されることによって通信端末を構成する通信ユニットであって、

インターネットを含まない１または複数の通信網に接続されるサーバの識別番号を記憶する記憶手段と、

前記識別番号を用いて前記サーバとの間で、インターネットを含まない１または複数の通信網を介した回線を接続する回線接続手段と、

前記回線を用いて秘匿を必要とする情報の通信を行う制御手段と、を具備することを特徴とする通信ユニット。

【請求項８】　請求項７記載の通信ユニットにおいて、

前記秘匿を必要とする情報がセッション鍵である

ことを特徴とする通信ユニット。

【請求項９】　請求項７記載の通信ユニットにおいて、

当該通信ユニットは、ＰＣカードの形体を有する

ことを特徴とする通信ユニット。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、例えばインターネットのように秘匿性の保証されていないネットワーク上での通信に用いて好適な通信システム、通信方法および通信ユニットに関する。

【０００２】

【従来の技術】

近年、インターネットの普及に伴って、様々な情報通信がインターネット上で行われている。インターネット上で通信される情報には、ホームページのように広く一般に公開する目的を有する情報もあれば、例えば商取引や個人情報などのように秘匿を必要とする情報もある。

しかしながら、インターネットの通信プロトコルであるＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）そのものには、データの改竄や

盗聴を防ぐセキュリティの仕組みは備わっていないため、インターネットにおいて行う通信は秘匿性が保証されていないのが実情である。

そこで、秘匿を必要とする情報を通信する技術として、暗号通信技術があり、これを利用してインターネット上においても専用線と同様の安全性および利便性を有する通信を実現するものが提案されていた。

【０００３】

【発明が解決しようとする課題】

ところで、この暗号通信をインターネットに利用する場合において、暗号化および復号の際の演算量が少なくて済む簡単な暗号を採用すると、暗号化および復号の処理負荷は少なくなるものの、第三者による暗号鍵の解読が容易に行われる可能性がある。その一方、十分な秘匿性を得るために複雑な暗号を採用すると、暗号化および復号の処理負荷が著しく高くなってしまい、迅速な通信を行うことが困難になる。このように、従来の技術の下では、秘匿性を確保し、かつ、迅速に所望の相手と通信を行うことが困難であった。

【０００４】

本発明は、以上説明した事情に鑑なみてなされたものであり、秘匿を必要とする情報の通信を高いセキュリティを維持し、かつ、迅速に行うことのできる通信システム、通信方法および通信ユニットを提供することを目的としている。

【０００５】

【課題を解決するための手段】

上述した課題を解決するため、請求項１記載の発明は、通信端末と、サーバとを具備し、

前記通信端末は、第１および第２の端末側通信手段を具備し、

前記サーバは、第１および第２のサーバ側通信手段を具備し、

前記通信端末の第１の端末側通信手段と前記サーバの第１のサーバ側通信手段は、インターネットを含まない１または複数の通信網を介して、秘匿を必要とする情報の通信を行い、

前記通信端末の第２の端末側通信手段と前記サーバの第２のサーバ側通信手段は、インターネットを含む１または複数の通信網を介して、秘匿を必要としない

情報の通信を行う

ことを特徴としている。

【０００６】

請求項２記載の発明は、通信端末と、サーバとを具備し、

前記通信端末は、第１および第２の端末側通信手段を具備し、

前記サーバは、第１および第２のサーバ側通信手段を具備し、

前記通信端末の第１の端末側通信手段と前記サーバの第１のサーバ側通信手段は、インターネットを含まない１または複数の通信網を介して、セッション鍵の交換を行い、

前記通信端末の第２の端末側通信手段と前記サーバの第２のサーバ側通信手段は、インターネットを含む１または複数の通信網を介して、前記セッション鍵によって暗号化された情報の通信を行う

ことを特徴としている。

【０００７】

請求項３記載の発明は、通信端末が、第１の通信手段により、インターネットを含まない１または複数の通信網を介して、前記サーバとの間で、秘匿を必要とする情報の通信を行う過程と、

前記通信端末が、前記第１の通信手段とは別の第２の通信手段により、インターネットを含む１または複数の通信網を介して、前記サーバとの間で、秘匿を必要としない情報の通信を行う過程と、を具備する

ことを特徴としている。

【０００８】

請求項４記載の発明は、通信端末が、第１の通信手段により、インターネットを含まない１または複数の通信網を介して、サーバとの間で、セッション鍵の交換を行う過程と、

前記通信端末が、前記第１の通信手段とは別の第２の通信手段により、インターネットを含む１または複数の通信網を介して、前記サーバとの間で、前記セッション鍵によって暗号化された情報の通信を行う過程と、を具備する

ことを特徴としている。

【０００９】

請求項５記載の発明は、通信端末が、第１の通信手段により、インターネットを含む１または複数の通信網を介して、電子ショップサーバとの間で、商品の購買を行い、購入した商品を指定した購買タグを受信する過程と、

前記通信端末が、前記第１の通信手段とは別の第２の通信手段により、インターネットを含まない１または複数の通信網を介して、前記電子ショップサーバとの間で、前記購買タグおよび秘匿を必要とする個人情報の通信を行う過程と、

前記電子ショップサーバが、前記購買タグおよび個人情報を用いて決済を行う過程と、を具備する

ことを特徴としている。

【００１０】

請求項６記載の発明は、通信端末が、第１の通信手段により、インターネットを含まない１または複数の通信網を介して、電子ショップサーバとの間で、セッション鍵の交換を行う過程と、

前記通信端末が、前記第１の通信手段とは別の第２の通信手段により、インターネットを含む１または複数の通信網を介して、前記電子ショップサーバとの間で、前記セッション鍵によって暗号化された情報で商品の購買を行い、購入した商品を指定した購買タグを記憶する過程と、

前記通信端末が、前記第１の通信手段により、インターネットを含まない１または複数の通信網を介して、前記電子ショップサーバとの間で、前記購買タグおよび秘匿を必要とする個人情報の通信を行う過程と、

前記電子ショップサーバが、前記購買タグおよび個人情報を用いて決済を行う過程と、を具備する

ことを特徴としている。

【００１１】

請求項７記載の発明は、外部ユニットに装着されることによって通信端末を構成する通信ユニットであって、

インターネットを含まない１または複数の通信網に接続されるサーバの識別番号を記憶する記憶手段と、

前記識別番号を用いて前記サーバとの間で、インターネットを含まない１または複数の通信網を介した回線を接続する回線接続手段と、

前記回線を用いて秘匿を必要とする情報の通信を行う制御手段と、を具備することを特徴としている。

【００１２】

請求項８記載の発明は、請求項７記載の通信ユニットにおいて、

前記秘匿を必要とする情報がセッション鍵である

ことを特徴としている。

【００１３】

請求項９記載の発明は、請求項７記載の通信ユニットにおいて、

当該通信ユニットは、ＰＣカードの形体を有する

ことを特徴としている。

【００１４】

【発明の実施の形態】

［Ａ．第１実施形態］

〈Ａ１〉通信システムの構成

〈Ａ１－１〉通信システムの全体構成

まず、図１は本発明の第１実施形態に係る通信システムの構成例を示す模式図である。

この通信システムは、同図に示すように、通信端末１０と、固定通信網１００と、インターネット２００と、移動通信網３００と、サーバ４００とによって大略構成されている。この通信システムにおいて、固定通信網１００および移動通信網３００は、盗聴などのおそれが比較的少なく安全性が高く、秘匿性が保証されているネットワークであるのに対して、インターネット２００は盗聴などのおそれが比較的多く安全性が低く、秘匿性が保証されていないネットワークである。そこで、本実施形態では、移動通信網３００を介して、通信端末１０とサーバ４００との間でセッション鍵の交換を行い、その後、固定通信網１００およびインターネット２００を介して、通信端末１０とサーバ４００との間で、このセッション鍵を用いた暗号通信を行う。

【００１５】

本実施形態では、暗号通信のための暗号化・復号方式として公開鍵暗号方式を採用し、セッション鍵として、この公開鍵暗号方式における公開鍵を使用する。

ここで、セッション鍵とは、１つのセッション（回線接続から回線接続断までの間）毎に使用される公開鍵のことである。

通信端末１０およびサーバ４００には、それぞれ複数の対をなす公開鍵と秘密鍵とが記憶されており、通信端末１０およびサーバ４００は、セッションの開始に先立って、互いにある公開鍵をセッション鍵として交換し、このセッション鍵に対応した秘密鍵を各自で保管する。

そして、セッションにおいて、通信端末１０では、サーバ４００から貰ったセッション鍵で暗号化した暗号信号を送信し、サーバ４００側から受信した暗号信号を秘密鍵で復号する。一方、サーバ４００では、通信端末１０から貰ったセッション鍵で暗号化した暗号信号を送信し、通信端末１０側から受信した暗号信号を秘密鍵で復号する。

このようなセッション鍵を用いた通信を通信端末１０とサーバ４００間で行うことにより、通信端末１０およびサーバ４００との間の通信に盗聴者が侵入するリプレーアタック等の不正が防止される。

【００１６】

〈Ａ１－２．通信端末の構成〉

通信端末１０は、無線通信ユニットたる通信用ＰＣカード５０を外部ユニットたるパソコン１１のカードスロット２０に装着することにより構成されている（図２参照）。この通信端末１０は、移動通信網３００を介してサーバ４００の第１ポート４０１に接続され、固定通信網１００およびインターネット２００を介してサーバ４００の第２ポート４０２に接続されるものである。

【００１７】

図３は、パーソナルコンピュータ１１（以下、パソコン１１という）およびＰＣカード５０の構成を示すブロック図である。

外部ユニットたるパソコン１１は、図３に示すように、ＣＰＵ１２と、ＲＯＭ（Read Only Memory）１３と、ＲＡＭ（Random Access Memory）１４と、ハ

ードディスク装置１５と、キー入力部１６と、表示部１７と、固定通信網１００に接続されるモデム１８と、カードスロット２０の奥部に設けられたコネクタ１９とによって大略構成されている。

ＲＯＭ１３は読み出し専用のプログラムメモリであり、ＣＰＵ１２はＲＯＭ１３から読出した制御プログラムを実行することにより、この通信端末１０の各部を制御するものである。ＲＡＭ１４は、ＣＰＵ１２が各種制御プログラムを実行する際のワークエリアとして用いられる。

【００１８】

ハードディスク装置１５には、各種プログラムや、ユーザが利用する各種情報が記憶されている。

このハードディスク装置１５に記憶されるプログラムには、例えば、パソコン１１を固定通信網１００を介してインターネット２００に接続するダイヤルアッププログラム、移動通信網３００を介して、ＰＣカード５０をサーバ４００に接続するプログラム、固定通信網１００およびインターネット２００を介して、モデム１８をサーバ４００に接続するプログラム、暗号通信用プログラム等がある。

【００１９】

ここで、ダイヤルアッププログラムとは、固定通信網１００をインターネット２００に接続する動作をＣＰＵ１２に行わせるものである。具体的には、パソコン１１を使用するユーザは、固定通信網１００とインターネット２００との間に接続されたプロバイダ（図示せず）に予め登録する。そして、固定通信網１００とインターネット２００とを接続するとき、通信端末１０がこの登録の際に貰う送信ユーザＩＤ（例えば、○○○△△）とパスワードをパソコン１１に入力する。パソコン１１のＣＰＵ１２は、この送信ユーザＩＤおよびパスワードを、モデム１８を介してプロバイダに送信する。プロバイダは、この送信ユーザＩＤとパスワードに基づいて認証処理を行い、固定通信網１００をインターネット２００に接続する。

暗号通信用プログラムとは、サーバ４００にセッション鍵の交換要求、公開鍵の送信、この公開鍵に対応した秘密鍵の記憶、サーバ４００から受信した公開鍵

（セッション鍵）の記憶、このセッション鍵を用いた情報の暗号化、受信した暗号信号の秘密鍵を用いた復号等、暗号通信に関する一連の動作をＣＰＵ１２に行わせるものである。

また、ハードディスク装置１５には、データテーブル１５Ａ（公開鍵（セッション鍵）ＰＯｋｅｙ１～ＰＯｋｅｙｎに対応した秘密鍵ＰＳｋｅｙ１～ＰＳｋｅｙｎ）（図５（ａ）参照）と、パソコン１１のＩＰアドレスＩＰａ、サーバ４００のＩＰアドレスＩＰｂ等が各種情報として記憶されている。

なお、パソコン１１は汎用のパーソナルコンピュータであり、ＰＡＤでもよい。

【００２０】

〈Ａ１－３〉無線通信ユニット（ＰＣカード）の構成

ＰＣカード５０は、記憶部５１と、コントローラ５２と、通信用送受信部５３と、アンテナ５４と、コネクタ５５とによって大略構成されている。

【００２１】

ここで、記憶部５１は、メモリ５１ＡおよびＩＤ記憶部５１Ｂからなり、メモリ５１Ａには、コントローラ５２で所定のオペレーティングシステムによりファイル管理を行うための汎用メモリの役割をなすエリアと、ＰＣカードの制御プログラムが格納されたエリアとがある。

ここで、所定のオペレーティングシステムとは、メモリ５１Ａ内のデータを用いて汎用ファイル管理が可能なもの、例えばMS-DOS、MS-Windows、Mac OS又はUNIX（いずれも登録商標）などとして知られるオペレーティングシステムをいう。このようなオペレーティングシステムを用いる場合、ＰＣカード５０においては、通常の電話帳や電子メールのログファイル等は、ＡＴＡフラッシュディスク上の汎用ファイルとして、パソコン１１により自由に読み書きが行われるものである。

また、ＩＤ記憶部５１Ｂには、ＰＣカード５０の識別番号ＩＤｃ（例えば電話番号）が記憶されると共に、サーバ４００の識別番号ＩＤｂ（電話番号）が記憶されている。

【００２２】

コントローラ５２は、メモリ５１Ａに記憶された制御プログラムを実行するものである。このコントローラ５２は、制御プログラムに従って、通信用送受信部５３で受信された信号をコネクタ５５に供給し、コネクタ５５で受信された信号を通信用送受信部５３に供給する。

【００２３】

通信用送受信部５３は、アンテナ５４を介して移動通信網３００に接続された基地局（図示せず）との間での通信が、例えばＰＤＣ（Personal Digital Cellular）若しくはＰＨＳ（Personal Handyphone System)によって行われるものである。

【００２４】

コネクタ５５は、パソコン１１のコネクタ１９に接続される接続用コネクタである。

ここで、コネクタ５５は、例えばコンパクトフラッシュ・タイプII（Compact Flash Type II）のような汎用性の高いコネクタで、上述したパソコン１１、その他の外部情報機器と接続するための外部インターフェースを構成している。なお、ＰＣカード５０のコネクタ５５は、上述のものに限定されるものではなく、ＰＣカード・スタンダード（PC Card Standard）等であってもよい。なお、ＰＣカード・スタンダードとは、ＪＥＩＤＡ（Japan Electronics Industry Development Association：日本電子工業振興協会）と米国ＰＣＭＣＩＡ（Personal Computer Memory Card International Association）が共同で制定した規格であり、厚さによって異なるタイプI、タイプII、タイプIII、タイプIV等がある。コンパクトフラッシュ（Compact Flash）・タイプは更に小型で、タイプIIは縦横が42.8×36.4、厚さが5.0(㎜)であり、これらをコネクタ５５として採用することにより、ＰＣカード５０の小型化が容易となる。

【００２５】

〈Ａ１－４．サーバの構成〉

サーバ４００は、図示しないルータを介してインターネット２００に接続されると共に、図示しない基地局を介して移動通信網３００に接続されたコンピュータである。

図４は、サーバ４００の構成を示すブロック図である。サーバ４００は、第１ポート４０１と、第２ポート４０２と、ＣＰＵ４０３と、ＲＯＭ４０４と、ＲＡＭ４０５と、ハードディスク装置４０６とによって大略構成されている。

【００２６】

第１ポート４０１は、図示しないアンテナ、通信用送受部等からなり、基地局を介して移動通信網３００に接続されている。そして、この第１ポート４０１は、図１に示す如く、移動通信網３００等を介して通信端末１０に接続される。

【００２７】

第２ポート４０２は、図示しないモデム、通信制御回路等からなり、ルータを介してインターネット２００に接続されている。この第２ポート４０２は、図１に示す如く、インターネット２００および固定通信網１００等を介して通信端末１０に接続される。

【００２８】

ＲＯＭ４０４は、制御プログラムを格納するプログラムメモリである。ＣＰＵ４０３は、ＲＯＭ４０４から読出した制御プログラムを実行することにより、サーバ４００全体を制御するものである。この際、ＲＡＭ４０５はＣＰＵ４０３のワークエリアとして用いられる。また、ＲＯＭ４０４には、サーバ４００の識別番号ＩＤｂ（例えば電話番号）およびＩＰアドレスＩＰｂが記憶されている。

【００２９】

ハードディスク装置４０６は、情報記憶部４０６Ａ、プログラム記憶部４０６Ｂおよび配信管理テーブル４０６Ｃという記憶エリアを有している。

情報記憶部４０６Ａには、通信端末１０に対して配信すべき情報を示す配信データが記憶される他、これらの情報のタイトルを通信端末１０の表示部１７に表示させるためのメニューデータ等が記憶されている。

【００３０】

記憶されたデータには、文字や記号を示すテキストデータ、音声や楽曲を示す音楽データ、静止画や動画を示す画像データ、ゲームソフト等のコンピュータプログラム等がある。これらのデータは、例えば音楽データはＭＰ３（MPEG Layer 3）形式、画像データはＧＩＦ（Graphics Interchange Format）形式、ＪＰＥＧ

(Joint Photographic Experts Group) 形式やＭＰＥＧ (Moving Picture Experts Group) 形式で、それぞれ適当な圧縮方式にて圧縮されたものである。

【００３１】

プログラム記憶部４０６Ｂには、情報配信プログラム、認証プログラム、移動通信網３００を介して、第１ポート４０１を通信端末１０のＰＣカード５０に接続するプログラム、固定通信網１００およびインターネット２００を介して、第２ポート４０２を通信端末１０のモデム１８に接続するプログラムおよび暗号通信用プログラム等が格納されている。

【００３２】

ここで、情報配信プログラムとは、通信端末１０から送信された要求情報に応じた配信情報の生成・送信をＣＰＵ４０３に行わせるものである。また、認証プログラムとは、配信管理テーブル４０６Ｃに記憶されたユーザＩＤ、パスワード等に基づいてユーザ認証をＣＰＵ４０３で行わせるものである。

暗号通信用プログラムとは、通信端末１０からセッション鍵の交換要求を受けた場合、公開鍵の送信、この公開鍵に対応した秘密鍵の記憶、通信端末１０から受信した公開鍵（セッション鍵）の記憶、このセッション鍵を用いた情報の暗号化、受信した暗号信号の秘密鍵を用いた復号等、暗号通信に関する一連の動作を、ＣＰＵ４０３に行わせるものである。

また、プログラム記憶部４０６Ｂには、図５（ｂ）に示すテーブルテーブル４０６Ｄ（公開鍵（セッション鍵）ＳＯｋｅｙ１～ＳＯｋｅｙｎに対応した秘密鍵ＳＳｋｅｙ１～ＳＳｋｅｙｎ）等が格納されている。

【００３３】

配信管理テーブル４０６Ｃには、予め登録されたユーザＩＤ、パスワード等が格納されている。これらの情報は、受信されたユーザＩＤおよびパスワードと比較され、通信端末１０（ユーザ）を特定するために用いられる。

【００３４】

〈Ａ２〉第１実施形態の動作

次に、上記構成を有する実施形態の動作について説明する。

【００３５】

図６に示すシーケンスチャートを参照しながら、本実施形態の動作について説明する。

【００３６】

まず、ユーザは、サーバ４００との間で情報の送受信を行うため、パソコン１１のキー入力部１６に、サーバ４００に予め登録したユーザＩＤおよびパスワード（以下、認証情報という）を入力する（ステップＳ１）。

【００３７】

パソコン１１のＣＰＵ１２は、制御プログラムに従って、この認証情報をＲＡＭ１４に記憶すると共に、認証情報をＰＣカード５０に送信する。

ＰＣカード５０のコントローラ５２は、メモリ５１Ａに記憶された制御プログラムに従って、サーバ４００の識別ＩＤｂを送信先、ＰＣカード５０の識別番号ＩＤｃを送信元として認証情報に付加し、この情報を通信用送受信部５３およびアンテナ５４を介して基地局に送信する。これにより、ユーザＩＤおよびパスワードを含む情報は、移動通信網３００を介してサーバ４００側の基地局に送信され、この基地局から第１ポート４０１（サーバ４００）に送信される（ステップＳ２）。

【００３８】

サーバ４００のＣＰＵ４０３は、認証情報を受けると、プログラム記憶部４０６Ｂに格納された認証プログラムを開始する。ＣＰＵ４０３は、このプログラムに基づき、第１ポート４０１から受信された認証情報のユーザＩＤおよびパスワードに対して認証処理を行う（ステップＳ３）。

【００３９】

ここで、ＣＰＵ４０３は、受信されたユーザＩＤおよびパスワードが予め配信管理テーブル４０６Ｃに記憶されたものでなかった場合（ステップＳ３；ＮＯ）には、この処理を終了する（ステップＳ４）。

【００４０】

一方、ＣＰＵ４０３は、受信されたユーザＩＤおよびパスワードが予め配信管理テーブル４０６Ｃに記憶されたものであった場合（ステップＳ３；ＹＥＳ）には、許可信号がＰＣカード５０（パソコン１１）に送信される。パソコン１１お

よびサーバ４００は、互いに接続するプログラムを開始する。このプログラムに従って、ＰＣカード５０とサーバ４００の第１ポート４０１との間に回線が張られ（ステップＳ５）、通信端末１０がサーバ４００に接続される。

【００４１】

次に、パソコン１１のＣＰＵ１２は、ハードディスク装置１５に記憶された暗号通信用プログラムが開始される。ＣＰＵ１２は、このプログラムに従って、セッション鍵の交換要求情報をＰＣカード５０に向けて送信する。

ＰＣカード５０のコントローラ５２は、制御プログラムに従って、サーバ４００の識別番号ＩＤｂを送信先、ＰＣカード５０の識別番号ＩＤｃを送信元として交換要求情報に付加し、この情報を通信用送受信部５３およびアンテナ５４を介して基地局に送信する。これにより、交換要求情報は、移動通信網３００（回線）を介してサーバ４００に送信される（ステップＳ６）。

【００４２】

パソコン１１のＣＰＵ１２は、暗号通信用プログラムに従って、ハードディスク装置１５に格納されたデータテーブル１５Ａからある公開鍵ＰＯｋｅｙ１をセッション鍵として選択し、このセッション鍵ＰＯｋｅｙ１をＰＣカード５０に向けて送信する。ＰＣカード５０のコントローラ５２は、セッション鍵ＰＯｋｅｙ１にサーバ４００の識別番号ＩＤｂを送信先、ＰＣカード５０の識別番号ＩＤｃを送信元として付加し、この情報を回線を介してサーバ４００に向けて送信する（ステップＳ７）。

また、サーバ４００のＣＰＵ４０３は、交換要求情報を受けて、プログラム記憶部４０６Ｂに格納された暗号通信用プログラムが開始される。

ＣＰＵ４０３は、このプログラムに従って、プログラム記憶部４０６Ｂに格納されたデータテーブル４０６Ｄからある公開鍵ＳＯｋｅｙ１をセッション鍵として選択し、このセッション鍵ＳＯｋｅｙ１にＰＣカード５０の識別番号ＩＤｃを送信先、サーバ４００の識別番号ＩＤｂを送信元として付加し、この情報を第１ポート４０１から移動通信網３００（回線）を介してＰＣカード５０に送信する（ステップＳ７′）。そして、ＰＣカード５０のコントローラ５２は、サーバ４００から送信されたセッション鍵ＳＯｋｅｙ１をパソコン１１に送信する。

【００４３】

パソコン１１のＣＰＵ１２は、回線およびＰＣカード５０を介して受信したサーバ４００のセッション鍵ＳＯｋｅｙ１をＲＡＭ１４に記憶すると共に、送信したセッション鍵ＰＯｋｅｙ１に対応した秘密鍵ＰＳｋｅｙ１をＲＡＭ１４に記憶する（ステップＳ８）。

サーバ４００のＣＰＵ４０３は、回線を介して受信したパソコン１１のセッション鍵ＰＯｋｅｙ１をＲＡＭ４０５に記憶すると共に、送信したセッション鍵ＳＯｋｅｙ１に対応した秘密鍵ＳＳｋｅｙ１を記憶する（ステップＳ９）。

【００４４】

そして、パソコン１０のＣＰＵ１２は、セッション鍵の交換が完了すると、回線を切断する信号をサーバ４００に送信し、回線の接続を切断する（ステップＳ１０）。

【００４５】

次に、通信端末１０とサーバ４００との間において、固定通信網１００およびインターネット２００を介して、秘匿を必要とする情報の授受する場合について説明する。

この処理に入る前に、前述したダイヤルアッププログラムを予め実行して固定通信網１００をインターネット２００に接続する。

次に、パソコン１１のＣＰＵ１２は、暗号通信用プログラムに従って、ＲＡＭ１４に記憶された認証情報（ユーザＩＤおよびパスワード）およびセッション鍵ＳＯｋｅｙ１を読出し、この認証情報をセッション鍵ＳＯｋｅｙ１で暗号化し（ステップＳ１１）、この暗号化した認証情報にサーバ４００のＩＰアドレスＩＰｂを送信先、パソコン１１のＩＰアドレスＩＰａを送信元として付加し、この暗号化された認証情報、モデム１８を介して固定通信網１００に送信する。これにより、暗号化された認証情報は、固定通信網１００およびインターネット２００を介してサーバ４００の第２ポート４０２に送信される（ステップＳ１２）。

【００４６】

サーバ４００のＣＰＵ４０３は、暗号化された認証情報を受けると、暗号通信用プログラムに従って、ＲＡＭ４０５に記憶された秘密鍵ＳＳｋｅｙ１を読出し

、この秘密鍵ＳＳｋｅｙ１で暗号化された認証情報を複合する（ステップＳ１３）。

そして、ＣＰＵ４０３は、認証プログラムに基づいて、復号された認証情報のユーザＩＤおよびパスワードに対して認証処理を行う（ステップＳ１４）。

【００４７】

ここで、ＣＰＵ４０３は、復号されたユーザＩＤおよびパスワードが予め配信管理テーブル４０６Ｃに記憶されたものでなかった場合（ステップＳ１４；ＮＯ）には、この処理を終了する（ステップＳ１５）。

【００４８】

一方、ＣＰＵ４０３は、復号されたユーザＩＤおよびパスワードが予め配信管理テーブル４０６Ｃに記憶されたものであった場合（ステップＳ１４；ＹＥＳ）には、許可信号がモデム１８（パソコン１１）に送信される。パソコン１１およびサーバ４００は、互いに接続するプログラムを開始する。このプログラムに従って、モデム１８とサーバ４００の第２ポート４０２との間が、固定通信網１００およびインターネット３００を介して接続される。

【００４９】

その後、通信端末１０とサーバ４００との間では、固定通信網１００およびインターネット３００を介して暗号通信による情報の授受を行う。

即ち、パソコン１１のＣＰＵ１２は、暗号通信用プログラムに基づいて、サーバ４００に送信する情報をＲＡＭ１４に記憶したセッション鍵ＳＯｋｅｙ１で暗号化し、サーバ４００に送信する（ステップＳ１７）。一方、ＣＰＵ１２は、受信したサーバ４００側からの暗号化された情報を、ＲＡＭ１４に記憶した秘密鍵ＰＳｋｅｙ１で復号する。

一方、サーバ４００のＣＰＵ４０３は、暗号通信用プログラムに基づいて、パソコン１１に送信する情報をＲＡＭ４０５に記憶したセッション鍵ＰＯｋｅｙ１で暗号化し、通信端末１０に送信する（ステップＳ１７′）。一方、ＣＰＵ４０３は、受信したパソコン１１側からの暗号化された情報を、ＲＡＭ４０５に記憶した秘密鍵ＳＳｋｅｙ１で復号する。

これにより、通信端末１０は、サーバ４００の情報記憶部４０６Ａに記憶され

たデータをセキュリティを高めて受信する。

【００５０】

そして、パソコン１０のＣＰＵ１２は、情報の授受が完了すると、通信を終了する（ステップＳ１８）。これに伴って、パソコン１１およびサーバ４００にそれぞれ記憶されたセッション鍵および秘密鍵を消去し、セッション鍵および秘密鍵を無効にする。なお、セッション鍵および秘密鍵に寿命を持たせることにより、自動的に無効にするものであってもよく、この場合固定通信網１００およびインターネット２００の接続を切断することなしに、鍵を消去することも可能となる。

【００５１】

〈Ａ３〉第１実施形態の効果

以上、述べたように、本実施形態による通信システムでは、移動通信網３００を介してセッション鍵の交換を行い、インターネット２００および固定通信網１００を介した通信時には、このセッション鍵を用いた暗号通信を行う。これにより、セキュリティの低いインターネット２００を含む１または複数の通信網を介して通信を行う場合であっても、情報の秘匿性を高めることができる。

【００５２】

［Ｂ．第２実施形態］

次に、本発明による第２実施形態に係る通信システムについて説明する。本実施形態では、この通信システムを電子商取引（ｅ－コマーズ：物品の購入）に適用した場合について述べる。

本実施形態の特徴は、秘匿を必要としない情報を固定通信網１００およびインターネット２００を含む通信網を用いて通信し、秘匿を必要とする情報をインターネットを含まない通信網を用いて通信した点にある。なお、本実施形態においては、前述した第１実施形態の通信システムとその基本構成が変わるところがないので、その説明を省略するものとする。

本実施形態におけるサーバ４００は、電子商取引を行うために電子ショップサーバとなり、このサーバ４００のハードディスク装置４０６には商品の情報や購買を行うためのプログラムが格納されることになる。

即ち、情報記憶部４０６Ａには、ユーザに対して販売する商品のメニューデータ、商品の情報データ等が記憶されている。なお、メニューデータとは、商品の写真や仕様等、各種情報および商品に対応した商品番号などである。

また、プログラム記憶部４０６Ｂには、情報配信プログラム、認証プログラムの他、商品購買プログラムおよび決済処理プログラム等が格納される。

ここで、商品購買プログラムとは、ユーザ毎にバスケット番号Ｂ１～Ｂｎを割り当て、このバスケット番号毎にユーザが購入を希望する商品の書き込みを、ＣＰＵ４０３に行わせるものである。

決済処理プログラムとは、ユーザからクレジット番号や商品の送付先等の個人情報が送信された段階で、バスケットに書き込まれた商品の金額をクレジット会社等に請求する等を、ＣＰＵ４０３に行わせるものである。

【００５３】

＜Ｂ１＞第２実施形態の動作

次に、上記構成を有する実施形態の動作について説明する。

【００５４】

図７に示すシーケンスチャートに基づき、本実施形態の動作について説明する。

まず、ユーザは、パソコン１１に前述したダイヤルアッププログラムを行わせるために、送信ユーザＩＤおよびパスワードをキー入力部１６から入力する。これにより、パソコン１１のＣＰＵ１２は、この送信ユーザＩＤおよびパスワードをプロバイダに送信し、固定通信網１００がインターネット２００に接続される。

【００５５】

また、本実施例では、送信ユーザＩＤをサーバ４００側での認証に用いるため、パソコン１１のＣＰＵ１２は、この送信ユーザＩＤに、サーバ４００のＩＰアドレスＩＰｂを送信先、パソコン１１のＩＰアドレスＩＰａを送信元として接続要求を固定通信網１００およびインターネット２００を介して送信する（ステップＳ２１）。

【００５６】

ここで、サーバ４００のＣＰＵ４０３は、プログラム記憶部４０６Ｂに格納された商品購買プログラムが実行される。ＣＰＵ４０３は、このプログラムに基づき、送信ユーザＩＤに対応したバスケット番号Ｂ１を割り振り、ＲＡＭ４０５に記憶する（ステップＳ２２）。

【００５７】

さらに、サーバ４００のＣＰＵ４０３は、情報記憶部４０６Ａのメニューデータを読出し、このメニューデータにパソコンのＩＰアドレスＩＰａを送信先、サーバ４００のＩＰアドレスＩＰｂを送信元として付加し、この情報をインターネット２００および固定通信網１００を介してパソコン１１に送信する（ステップＳ２３）。

【００５８】

パソコン１１のＣＰＵ１２は、受信したメニューデータを表示部１７に表示する。これにより、ユーザはサーバ４００が販売している商品を把握する。

ユーザは、パソコン１１の表示部１７のメニューを参照しつつ、所望の商品を選択する。即ち、ユーザが予め決められた選択動作を行うことにより、ＣＰＵ１２は、ユーザが選択した商品の番号（例えば、ｄｄｄ）を固定通信網１００およびインターネット２００を介してサーバ４００に送信する（ステップＳ２４）。予め決められた選択動作とは、例えば、表示部１７に表示される商品の写真をマウスのポインタでクリックする、といった具合である。そして、サーバ４００のＣＰＵ４０３は、対応したバスケットＢ１に選択された商品番号ｄｄｄを書き込む。

ユーザが商品の選択を終了すると、パソコン１１に予め決められた信号がユーザによって入力されることにより、パソコン１１のＣＰＵ１２は、選択終了信号を固定通信網１００およびインターネット２００を介してサーバ４００に送信する。

【００５９】

サーバ４００のＣＰＵ４０３は、この選択終了信号を受けて、送信ユーザＩＤに対応付けて購買タグ（バスケット番号Ｂ１＋商品番号ｄｄｄ）をＲＡＭ４０５に記憶する（ステップＳ２５）。さらに、サーバ４００のＣＰＵ４０３は、この

購買タグにパソコンのＩＰアドレスＩＰａを送信先、サーバ４００のＩＰアドレスＩＰｂを送信元として付加し、この情報を固定通信網１００およびインターネット２００を介してパソコン１１に送信する（ステップＳ２６）。

【００６０】

パソコン１１のＣＰＵ１２は、この購買タグをＲＡＭ１４に記憶する（ステップＳ２７）。そして、パソコン１０のＣＰＵ１２は、商品の購買処理が終わると、固定通信網１００およびインターネット２００による通信を終了する（ステップＳ２８）。

【００６１】

次に、ユーザは、サーバ４００にクレジット番号、商品の送信先住所等の個人情報を送信するために、パソコン１１のキー入力部１６に個人情報を入力する（ステップＳ２９）。この個人情報とは、盗聴されては困る情報である。

【００６２】

パソコン１１のＣＰＵ１２は、制御プログラムに従って、購買タグをＲＡＭ１４から読出し、この購買タグをＰＣカード５０に送信する。

ＰＣカード５０のコントローラ５２は、メモリ５１Ａに記憶された制御プログラムに従って、サーバ４００の識別番号ＩＤｂを送信先、ＰＣカード５０の識別番号ＩＤｃを送信元として購買タグに付加し、この情報を通信用送受信部５３およびアンテナ５４を介して基地局に送信する。これにより、購買タグは、移動通信網３００を介してサーバ４００側の基地局に送信され、この基地局から第１ポート４０１（サーバ４００）に送信される（ステップＳ３０）。

【００６３】

サーバ４００のＣＰＵ４０３は、購買タグを受けると、プログラム記憶部４０６Ｂに格納された認証プログラムが開始される。ＣＰＵ４０３は、このプログラムに基づき、第１ポート４０１から受信された購買タグに対して認証処理を行う（ステップＳ３１）。

【００６４】

ここで、ＣＰＵ４０３は、受信された購買タグがＲＡＭ４０５に記憶されたものでなかった場合（ステップＳ３１；ＮＯ）には、この処理を終了する（ステッ

プＳ３２）。

【００６５】

一方、ＣＰＵ４０３は、受信された購買タグがＲＡＭ４０５に記憶されたものであった場合（ステップＳ３０；ＹＥＳ）には、許可信号がＰＣカード５０（パソコン１１）に送信される。パソコン１１およびサーバ４００は、互いに接続するプログラムを開始する。このプログラムに従って、ＰＣカード５０とサーバ４００の第１ポート４０１との間に回線が張られ（ステップＳ３３）、通信端末１０がサーバ４００に接続される。

【００６６】

次に、パソコン１１のＣＰＵ１２は、制御プログラムに従って、個人情報をＰＣカード５０に送信する。

ＰＣカード５０のコントローラ５２は、メモリ５１Ａに記憶された制御プログラムに従って、サーバ４００の識別ＩＤｂを送信先、ＰＣカード５０の識別番号ＩＤｃを送信元として個人情報に付加し、この情報を通信用送受信部５３およびアンテナ５４を介して基地局に送信する。これにより、個人情報は、移動通信網３００を介してサーバ４００側の基地局に送信され、この基地局から第１ポート４０１（サーバ４００）に送信される（ステップＳ３４）

【００６７】

サーバ４００のＣＰＵ４０３は、この個人情報を受けて、決済処理を行う（ステップＳ３５）。この場合、クレジット会社に商品ｄｄｄの金額を請求すると共に、商品ｄｄｄを送信先住所に発送する手続き等を行う。

【００６８】

そして、パソコン１０のＣＰＵ１２は、個人情報の送信等が終了すると、回線の接続を断つ信号をサーバ４００に送信し、回線を切断する（ステップＳ３６）。

【００６９】

〈Ｂ２〉第２実施形態の効果

以上、述べたように、本実施形態による通信システムでは、固定通信網１００およびインターネット２００を介した通信によって商品の選択を行い、移動通信

網２００を介した通信によって秘匿を必要とする個人情報を送信するようにした。これにより、盗聴者が個人情報を盗聴するのを防止でき、個人情報等の秘匿性を高めることができる。

【００７０】

[C．第３実施形態]

次に、本発明による第３実施形態に係る通信システムについて説明する。本実施形態においては、この通信システムを電子商取引（ｅ－コマーズ：物品の購入）に適用した場合を例示する。

本実施形態の特徴は、インターネットを含まない通信網を介してセッション鍵の交換を行い、インターネットを含む通信網を介してこのセッション鍵を用いた通信を行い、最後に個人情報をインターネットを含まない通信網を介して通信した点にある。なお、本実施形態においては、前述した第１実施形態の通信システムとその構成は変わるところがないので、その説明を省略するものとする。

本実施形態におけるサーバ４００は、電子商取引では電子ショップサーバなる。このため、サーバ４００のハードディスク装置４０６には、商品の情報や購買を行うためのプログラムが格納されることになる。

即ち、情報記憶部４０６Ａには、ユーザに対して販売する商品のメニューデータ、商品の情報データ等が記憶されている。なお、メニューデータとは、商品の写真や仕様等、各種情報および商品に対応した商品番号などである。

また、プログラム記憶部４０６Ｂには、情報配信プログラム、認証プログラムの他、商品購買プログラムおよび決済処理プログラム等が格納されている。

ここで、商品購買プログラムとは、ユーザ毎にバスケット番号Ｂ１～Ｂｎを割り当て、このバスケット番号毎にユーザが購入を希望する商品の書き込みを、ＣＰＵ４０３に行わせるものである。

決済処理プログラムとは、ユーザからクレジット番号や商品の送付先等の個人情報が送信された段階で、バスケットに書き込まれた商品の金額をカード会社に請求書を発行する等を、ＣＰＵ４０３に行わせるものである。

【００７１】

〈Ｃ１〉第３実施形態の動作

次に、上記構成を有する実施形態の動作について説明する。

【００７２】

図８および図９に示すシーケンスチャートを参照しながら、本実施形態の動作について説明する。

【００７３】

まず、ユーザは、パソコン１１のキー入力部１６に、サーバ４００に予め登録したユーザＩＤおよびパスワード（以下、認証情報という）を入力する（ステップＳ４１）。

【００７４】

パソコン１１のＣＰＵ１２は、制御プログラムに従って、この認証情報をＲＡＭ１４に記憶すると共に、認証情報をＰＣカード５０に送信する。

ＰＣカード５０のコントローラ５２は、メモリ５１Ａに記憶された制御プログラムに従って、サーバ４００の識別番号ＩＤｂを送信先、ＰＣカード５０の識別番号ＩＤｃを送信元として認証情報に付加し、この情報を通信用送受信部５３およびアンテナ５４を介して基地局に送信する。これにより、ユーザＩＤおよびパスワードを含む情報は、移動通信網３００を介してサーバ４００側の基地局に送信され、この基地局から第１ポート４０１（サーバ４００）に送信される（ステップＳ４２）。

【００７５】

サーバ４００のＣＰＵ４０３は、認証情報を受けると、プログラム記憶部４０６Ｂに格納された認証プログラムを開始する。ＣＰＵ４０３は、このプログラムに基づき、第１ポート４０１から受信された認証情報のユーザＩＤおよびパスワードに対して認証処理を行う（ステップＳ４３）。

【００７６】

ここで、ＣＰＵ４０３は、受信されたユーザＩＤおよびパスワードが予め配信管理テーブル４０６Ｃに記憶されたものでなかった場合（ステップＳ４３；ＮＯ）には、この処理を終了する（ステップＳ４４）。

【００７７】

一方、ＣＰＵ４０３は、受信されたユーザＩＤおよびパスワードが予め配信管

理テーブル４０６Ｃに記憶されたものであった場合（ステップＳ４３；ＹＥＳ）には、許可信号がＰＣカード５０（パソコン１１）に送信される。パソコン１１およびサーバ４００は、互いに接続するプログラムを開始する。このプログラムに従って、ＰＣカード５０とサーバ４００の第１ポート４０１との間にダイヤル回線が張られ（ステップＳ４５）、通信端末１０がサーバ４００に接続される。

【００７８】

次に、パソコン１１のＣＰＵ１２は、ハードディスク装置１５に記憶された暗号通信用プログラムが開始される。ＣＰＵ１２は、このプログラムに従って、セッション鍵の交換要求情報をＰＣカード５０に向けて送信する。

ＰＣカード５０のコントローラ５２は、制御プログラムに従って、サーバ４００の識別番号ＩＤｂを送信先、ＰＣカード５０の識別番号ＩＤｃを送信元として交換要求情報に付加し、この情報を通信用送受信部５３およびアンテナ５４を介して基地局に送信する。これにより、交換要求情報は、移動通信網３００（回線）を介してサーバ４００に送信される（ステップＳ４６）。

【００７９】

パソコン１１のＣＰＵ１２は、暗号通信用プログラムに従って、ハードディスク装置１５に格納されたデータテーブル１５Ａからある公開鍵ＰＯｋｅｙ１をセッション鍵として選択し、このセッション鍵ＰＯｋｅｙ１をＰＣカード５０に向けて送信する。ＰＣカード５０のコントローラ５２は、セッション鍵ＰＯｋｅｙ１にサーバ４００の識別番号ＩＤｂを送信先、ＰＣカード５０の識別番号ＩＤｃを送信元として付加し、この情報を回線を介してサーバ４００に向けて送信する（ステップＳ４７）。

また、サーバ４００のＣＰＵ４０３は、交換要求情報を受けて、プログラム記憶部４０６Ｂに格納された暗号通信用プログラムが開始される。

ＣＰＵ４０３は、このプログラムに従って、プログラム記憶部４０６Ｂに格納されたデータテーブル４０６Ｄからある公開鍵ＳＯｋｅｙ１をセッション鍵として選択し、このセッション鍵ＳＯｋｅｙ１にＰＣカード５０の識別番号ＩＤｃを送信先、サーバ４００の識別番号ＩＤｂを送信元として付加し、この情報を第１ポート４０１から移動通信網３００（回線）を介してＰＣカード５０に送信する

（ステップＳ４７′）。

そして、ＰＣカード５０のコントローラ５２は、サーバ４００から送信されたセッション鍵ＳＯｋｅｙ１をパソコン１１に送信する。

【００８０】

パソコン１１のＣＰＵ１２は、回線およびＰＣカード５０を介して受信したサーバ４００のセッション鍵ＳＯｋｅｙ１をＲＡＭ１４に記憶すると共に、送信したセッション鍵ＰＯｋｅｙ１に対応した秘密鍵ＰＳｋｅｙ１をＲＡＭ１４に記憶する（ステップＳ４８）。

サーバ４００のＣＰＵ４０３は、回線を介して受信したパソコン１１のセッション鍵ＰＯｋｅｙ１をＲＡＭ４０５に記憶すると共に、送信したセッション鍵ＳＯｋｅｙ１に対応した秘密鍵ＳＳｋｅｙ１を記憶する（ステップＳ４９）。

【００８１】

そして、パソコン１０のＣＰＵ１２は、セッション鍵の交換が完了すると、回線の接続を断つ信号をサーバ４００に送信し、回線を切断する（ステップＳ５０）。

【００８２】

次に、前述した処理によって取得したセッション鍵を用いた暗号通信を固定通信網１００およびインターネット２００を介して行う。この処理に入る前に、前述したダイヤルアッププログラムを予め実行して固定通信網１００をインターネット２００に接続する。

次に、パソコン１１のＣＰＵ１２は、暗号通信用プログラムに従って、ＲＡＭ１４に記憶された認証情報（ユーザＩＤおよびパスワード）およびセッション鍵ＳＯｋｅｙ１を読出し、この認証情報をセッション鍵ＳＯｋｅｙ１で暗号化し（ステップＳ５１）、この暗号化した認証情報にサーバ４００のＩＰアドレスＩＰｂを送信先、パソコン１１のＩＰアドレスＩＰａを送信元として付加し、この暗号化された認証情報を、モデム１８を介して固定通信網１００に送信する。これにより、暗号化された認証情報は、固定通信網１００およびインターネット２００を介してサーバ４００の第２ポート４０２に送信される（ステップＳ５２）。

【００８３】

サーバ４００のＣＰＵ４０３は、暗号化された認証情報を受けると、暗号通信用プログラムに従って、ＲＡＭ４０５に記憶された秘密鍵ＳＳｋｅｙ１を読出し、この秘密鍵ＳＳｋｅｙ１で暗号化された認証情報を複合する（ステップＳ５３）。

そして、ＣＰＵ４０３は、認証プログラムに基づいて、復号された認証情報のユーザＩＤおよびパスワードに対して認証処理を行う（ステップＳ５４）。

【００８４】

ここで、ＣＰＵ４０３は、復号されたユーザＩＤおよびパスワードが予め配信管理テーブル４０６Ｃに記憶されたものでなかった場合（ステップＳ５４；ＮＯ）には、この処理を終了する（ステップＳ５５）。

【００８５】

一方、ＣＰＵ４０３は、復号されたユーザＩＤおよびパスワードが予め配信管理テーブル４０６Ｃに記憶されたものであった場合（ステップＳ５４；ＹＥＳ）には、許可信号がモデム１８（パソコン１１）に送信される。パソコン１１およびサーバ４００は、互いに接続するプログラムを開始する。このプログラムに従って、モデム１８およびサーバ４００の第２ポート４０２とが、固定通信網１００およびインターネット２００を介して接続される。

【００８６】

その後、通信端末１０とサーバ４００との間では、固定通信網１００およびインターネット２００を用いて暗号通信を行うことになる（ステップＳ５７、Ｓ５８、Ｓ６０）。

【００８７】

ここで、サーバ４００のＣＰＵ４０３は、プログラム記憶部４０６Ｂに格納された商品購買プログラムを実行する。ＣＰＵ４０３は、このプログラムに基づき、ユーザＩＤに対応したバスケット番号Ｂ１を割り振り、ＲＡＭ４０５に記憶する（ステップＳ５６）。

【００８８】

さらに、サーバ４００のＣＰＵ４０３は、情報記憶部４０６Ａのメニューデータを読出し、このメニューデータをセッション鍵ＰＯｋｅｙ１で暗号化し、この

暗号化したメニューデータにパソコンのＩＰアドレスＩＰａを送信先、サーバ４００のＩＰアドレスＩＰｂを送信元として付加し、この情報を固定通信網１００およびインターネット２００を介してパソコン１１に送信する（ステップＳ５７）。

【００８９】

パソコン１１のＣＰＵ１２は、受信したメニューデータを秘密鍵ＰＳｋｅｙ１で復号し、この復号したメニューデータを表示部１７に表示する。これにより、ユーザはサーバ４００が販売している商品を把握する。

ユーザは、パソコン１１の表示部１７のメニューを参照しつつ、所望の商品を選択する。即ち、予め決められた選択動作によって、ユーザが選択した商品の番号（例えば、ｄｄｄ）を選択した場合、パソコン１１のＣＰＵ１２は、暗号通信用プログラムに従って、商品番号ｄｄｄをセッション鍵ＳＯｋｅｙ１で暗号化し、この暗号化した商品番号にサーバ４００のＩＰアドレスＩＰｂを送信先、パソコン１１のＩＰアドレスＩＰａを送信元として付加し、この暗号化された商品番号を、モデム１８を介して固定通信網１００に送信する。これにより、暗号化された商品番号は、固定通信網１００およびインターネット２００を介してサーバ４００の第２ポート４０２に送信される（ステップＳ５８）。

予め決められた選択動作とは、例えば、表示部１７に表示される商品の写真をマウスのポインタでクリックする、といった具合である。

そして、サーバ４００のＣＰＵ４０３は、暗号化された商品番号を受けると、暗号通信用プログラムに従って、ＲＡＭ４０５に記憶された秘密鍵ＳＳｋｅｙ１を読出し、この秘密鍵ＳＳｋｅｙ１で暗号化された商品番号を複合する。そして、ＣＰＵ４０３は、復号された商品番号ｄｄｄを、対応したバスケットＢ１に順次書き込む。

ユーザが商品の選択を終了すると、パソコン１１に予め決められた信号がユーザによって入力されることにより、パソコン１１のＣＰＵ１２は、選択終了信号を固定通信網１００およびインターネット２００を介してサーバ４００に送信する。

【００９０】

サーバ４００のＣＰＵ４０３は、この選択終了信号を受けて、ユーザＩＤに対応付けて購買タグ（バスケット番号Ｂ１＋商品番号ｄｄｄ）をＲＡＭ４０５に記憶する（ステップＳ５９）。さらに、サーバ４００のＣＰＵ４０３は、セッション鍵ＰＯｋｅｙ１で暗号化し、この暗号化した購買タグにパソコンのＩＰアドレスＩＰａを送信先、サーバ４００のＩＰアドレスＩＰｂを送信元として付加し、この情報を固定通信網１００およびインターネット２００を介してパソコン１１に送信する（ステップＳ６０）。

【００９１】

パソコン１１のＣＰＵ１２は、受信した購買タグを秘密鍵ＰＳｋｅｙ１で復号し、復号した購買タグをＲＡＭ１４に記憶する（ステップＳ６１）。そして、パソコン１０のＣＰＵ１２は、商品の購買処理が終わると、通信を終了する（ステップＳ６２）。

【００９２】

次に、ユーザは、サーバ４００にクレジット番号、商品の送信先住所等の個人情報を送信するために、キー入力部１６に個人情報を入力する（ステップＳ６３）。この個人情報とは、盗聴されては困る情報である。

【００９３】

パソコン１１のＣＰＵ１２は、制御プログラムに従って、購買タグをＲＡＭ１４から読出し、この購買タグをＰＣカード５０に送信する。

ＰＣカード５０のコントローラ５２は、メモリ５１Ａに記憶された制御プログラムに従って、サーバ４００の識別ＩＤｂを送信先、ＰＣカード５０の識別番号ＩＤｃを送信元として購買タグに付加し、この情報を通信用送受信部５３およびアンテナ５４を介して基地局に送信する。これにより、購買タグは、移動通信網３００を介してサーバ４００側の基地局に送信され、この基地局から第１ポート４０１（サーバ４００）に送信される（ステップＳ６４）。

【００９４】

サーバ４００のＣＰＵ４０３は、購買タグを受けると、プログラム記憶部４０６Ｂに格納された認証プログラムが開始される。ＣＰＵ４０３は、このプログラムに基づき、第１ポート４０１から受信された購買タグに対して認証処理を行う

（ステップＳ６５）。

【００９５】

ここで、ＣＰＵ４０３は、受信された購買タグがＲＡＭ４０５に記憶されたものでなかった場合（ステップＳ６５；ＮＯ）には、この処理を終了する（ステップＳ６６）。

【００９６】

一方、ＣＰＵ４０３は、受信された購買タグがＲＡＭ４０５に記憶されたものであった場合（ステップＳ６５；ＹＥＳ）には、許可信号がＰＣカード５０（パソコン１１）に送信される。パソコン１１とサーバ４００との間には、移動通信網３００を介してダイヤル回線が張られ（ステップＳ６７）、通信端末１０がサーバ４００に接続される。

【００９７】

次に、パソコン１１のＣＰＵ１２は、制御プログラムに従って、個人情報をＰＣカード５０に送信する。

ＰＣカード５０のコントローラ５２は、メモリ５１Ａに記憶された制御プログラムに従って、サーバ４００の識別ＩＤｂを送信先、ＰＣカード５０の識別番号ＩＤｃを送信元として個人情報に付加し、この情報を通信用送受信部５３およびアンテナ５４を介して基地局に送信する。これにより、個人情報は、移動通信網３００を介してサーバ４００側の基地局に送信され、この基地局から第１ポート４０１（サーバ４００）に送信される（ステップＳ６８）

【００９８】

サーバ４００のＣＰＵ４０３は、この個人情報を受けて、決済処理を行う（ステップＳ６９）。この場合、クレジット会社に商品ｄｄｄの金額を請求すると共に、商品ｄｄｄを送信先住所に発送する手続き等を行う。

【００９９】

そして、パソコン１０のＣＰＵ１２は、個人情報の送信等が終了すると、ダイヤル回線の接続を断つ信号をサーバ４００に送信し、回線を切断する（ステップＳ７０）。

【０１００】

〈Ｃ２〉第３実施形態の効果

以上、述べたように、本実施形態による通信システムでは、固定通信網１００およびインターネット２００を介して商品の選択を行う場合、予めセキュリティの高い移動通信網３００を介してセッション鍵を交換し、このセッション鍵を用いて固定通信網１００およびインターネット２００を介した通信を行うようにした。これにより、盗聴者が個人情報を盗聴するのを防止でき、個人情報等の秘匿性を高めることができる。

しかも、本実施形態では、固定通信網１００およびインターネット２００による通信をセッション鍵によって暗号化して行っているため、購買タグを盗聴者が盗聴するのを防止でき、同じ製品を先回りして買われてしまうのを防止することができる。また、この方式は、１つの製品を買うオークション等の場合に、特に有効である。

【０１０１】

［Ｄ．変形例］

〈Ｄ－１〉

前記各実施形態では、固定通信網１００およびインターネット２００を介して秘匿を必要としない情報の通信を行い、移動通信網３００を介して秘匿を必要とする情報の通信を行うようにしたが、本発明はこれに限らず、図１０に示すように、固定通信網１００およびインターネット２００を介して秘匿を必要としない情報の通信を行い、移動通信網３００および固定通信網１００を介して秘匿を必要とする情報の通信を行うにしもよく、また図１１に示すように、移動通信網３００およびインターネット２００を介して秘匿を必要としない情報の通信を行い、移動通信網３００を介して秘匿を必要とする情報の通信を行うにしてもよい。

【０１０２】

〈Ｄ－２〉

前記第１、第３実施形態では、固定通信網１００およびインターネット２００で暗号通信を行う場合、１個のセッション鍵を用いて暗号化するようにしたが、２個以上のセッション鍵をダイヤル回線を用いて交換し、これらのセッション鍵によって暗号化することも可能である。

【０１０３】

〈Ｄ－３〉

前記第２、第３実施形態では、購買タグがサーバ４００から通信端末１０に送信された後に、固定通信網１００およびインターネット２００を介した通信を終了するようにしていたが、終了した後でも、一定時間内に通信端末１０側から購買タグがサーバ４００に向けて送信されることにより、商品の追加、削除等の変更を可能としてもよい。この場合には、個人情報がユーザから入力されるまでの間、この処理を可能にしてもよく、またタイマを作動させてこの処理を行わせるようにしてもよい。

【０１０４】

〈Ｄ－４〉

前記各実施形態における通信は、例えばパケット通信方式によって行うようにしていもよい。

【０１０５】

〈Ｄ－５〉

前記無線端末１０は、パソコン１１のカードスロット２０にＰＣカード５０を装着することによって構成したが、本発明はこれに限らず、パソコン１１に携帯電話またはＰＨＳを接続したものであってもよい。本発明を構成する通信端末は２つの通信手段を備えたものであればよい。

【０１０６】

【発明の効果】

上述したように本発明によれば、秘匿を必要とする情報の通信を高いセキュリティを維持し、かつ、迅速に行うことができる。

【図面の簡単な説明】

【図１】

本発明の第１実施形態に係る通信システムの概略構成を示すブロック図である。

【図２】

同実施形態に係る通信端末を構成するパソコンと無線通信ユニット（ＰＣカー

ド）とを示す斜視図である。

【図３】

同実施形態に係るパソコンおよびＰＣカードの概略構成を示すブロック図である。

【図４】

同実施形態に係るサーバの構成の概略構成を示すブロック図である。

【図５】

同実施形態に用いられるセッション鍵に対する秘密鍵を示したデータテーブルである。

【図６】

同実施形態による通信システムの動作を示すシーケンスチャートである。

【図７】

第２実施形態による通信システムの動作を示すシーケンスチャートである。

【図８】

第３実施形態による通信システムの動作を示すシーケンスチャートである。

【図９】

同実施形態による通信システムの動作を示す図８に続くシーケンスチャートである。

【図１０】

本発明の変形例による通信システムの概略構成を示すブロック図である。

【図１１】

本発明の他の変形例による通信システムの概略構成を示すブロック図である。

【符号の説明】

１０・・・通信端末

１１・・・パソコン

１８・・・モデム

５０・・・ＰＣカード

１００・・・固定通信網

２００・・・インターネット

３００・・・移動通信網

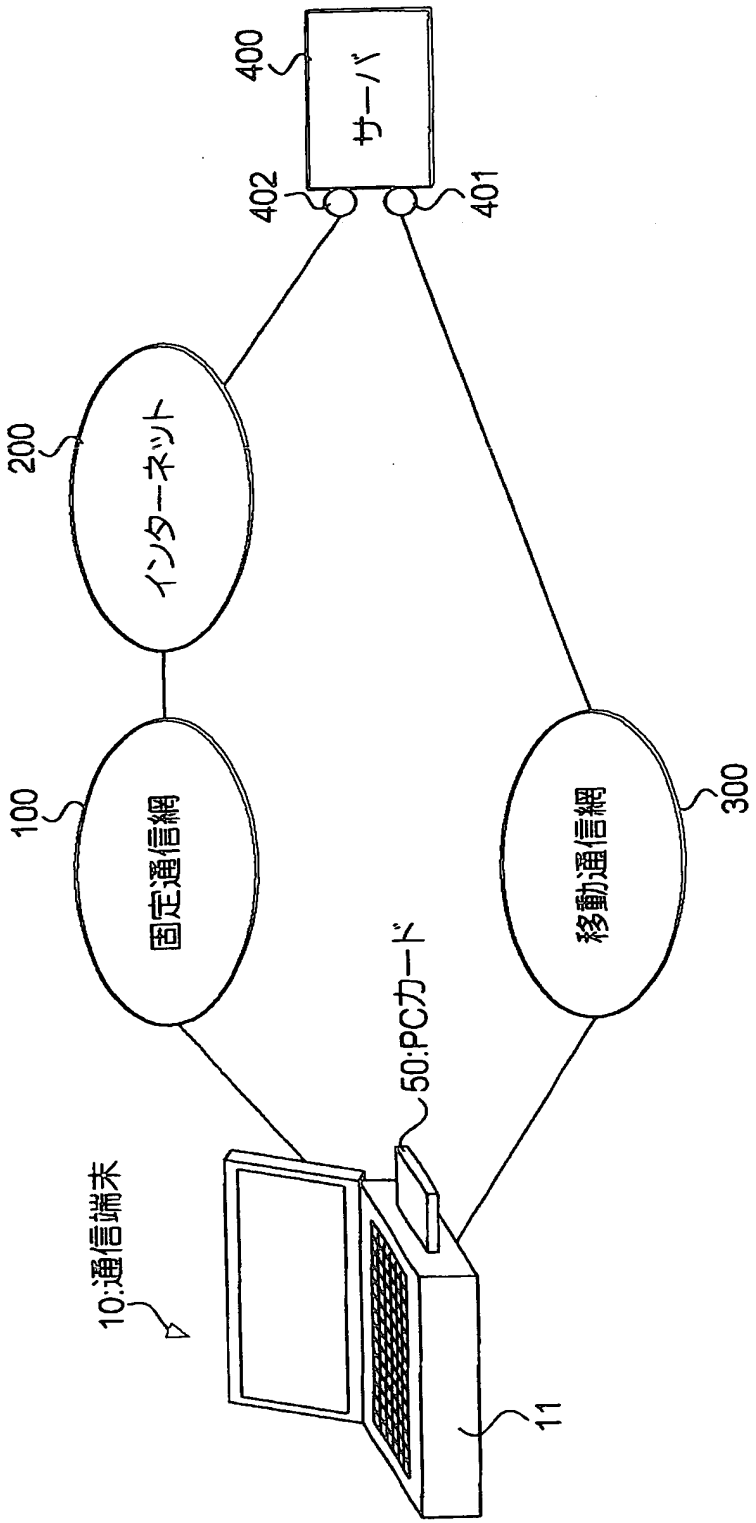
４００・・・サーバ

４０１・・・第１ポート

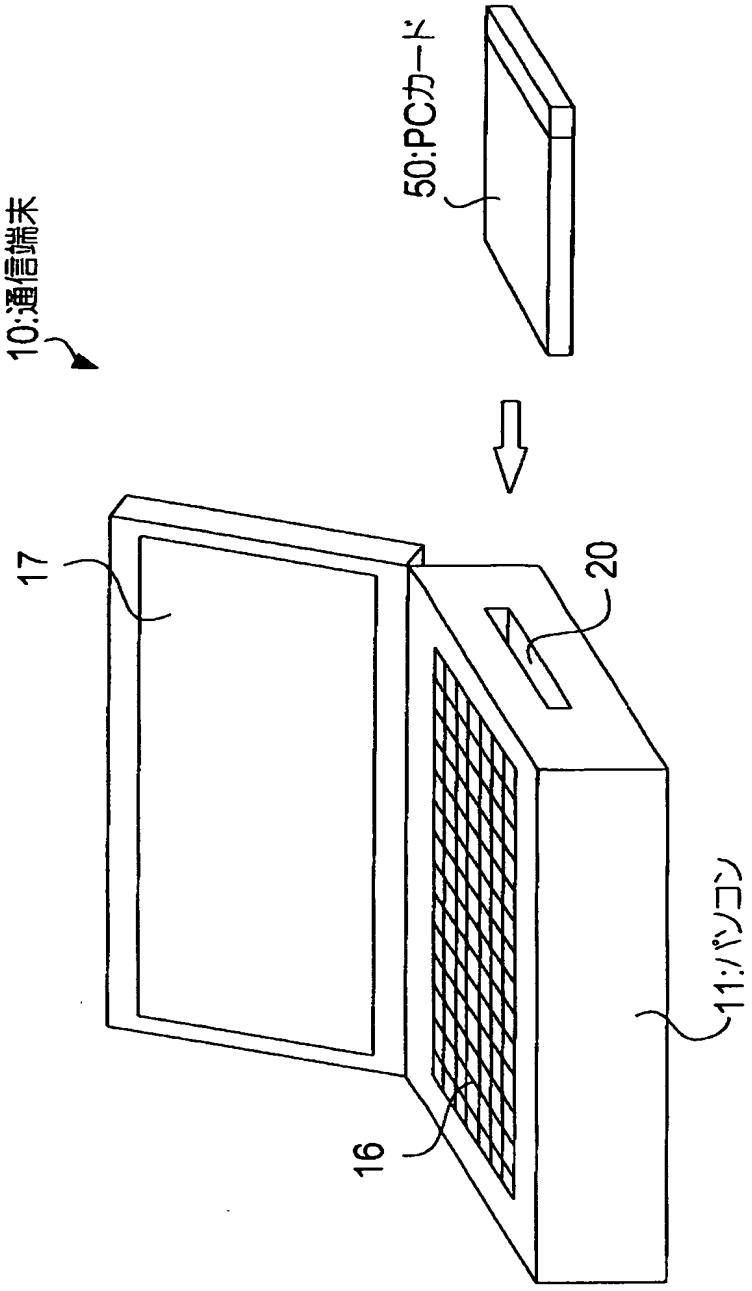
４０２・・・第２ポート

【書類名】　図面

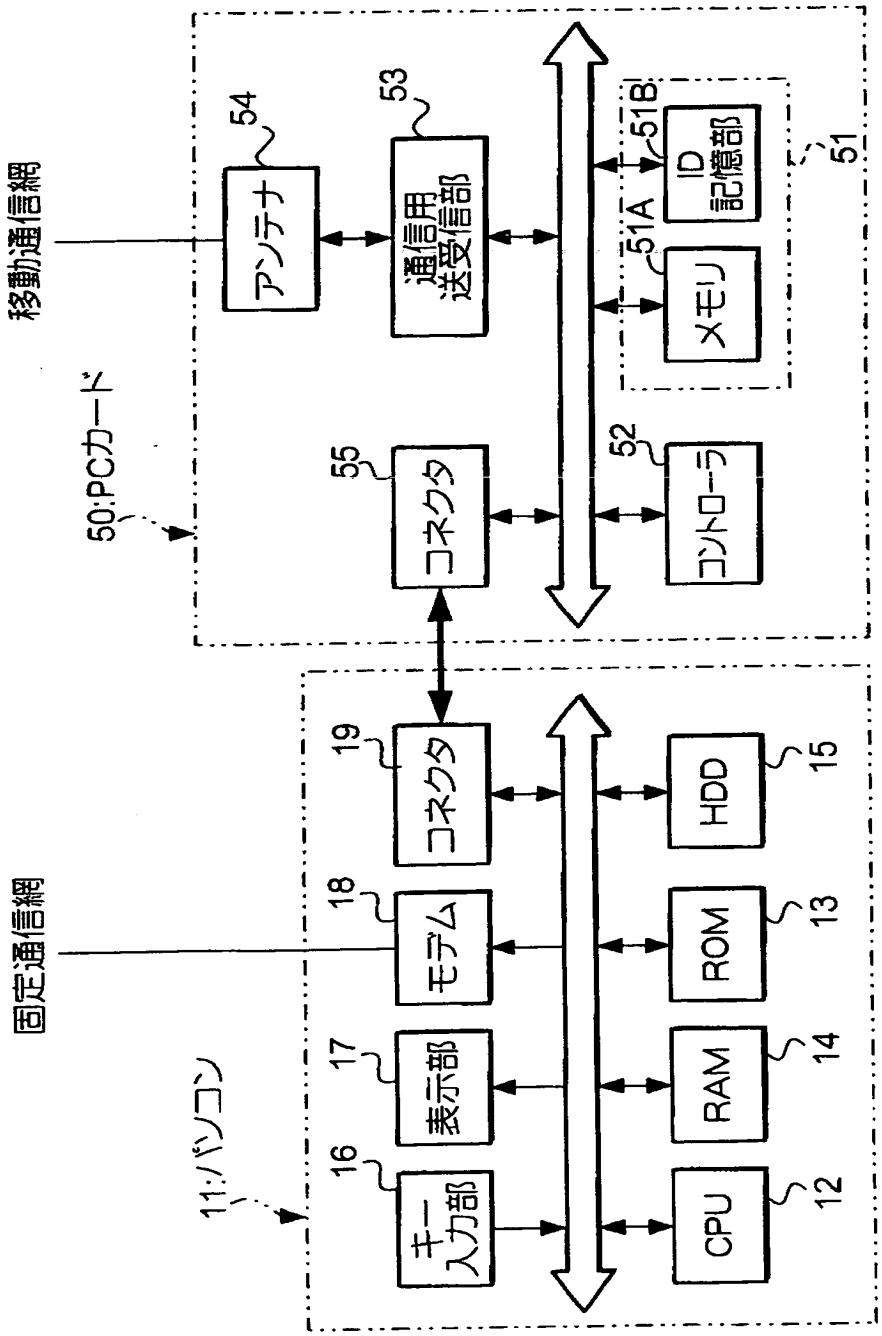
【図１】


400
サーバ
402
401
200
インターネット
100
固定通信網
300
移動通信網
50:PCカード
10:通信端末
11

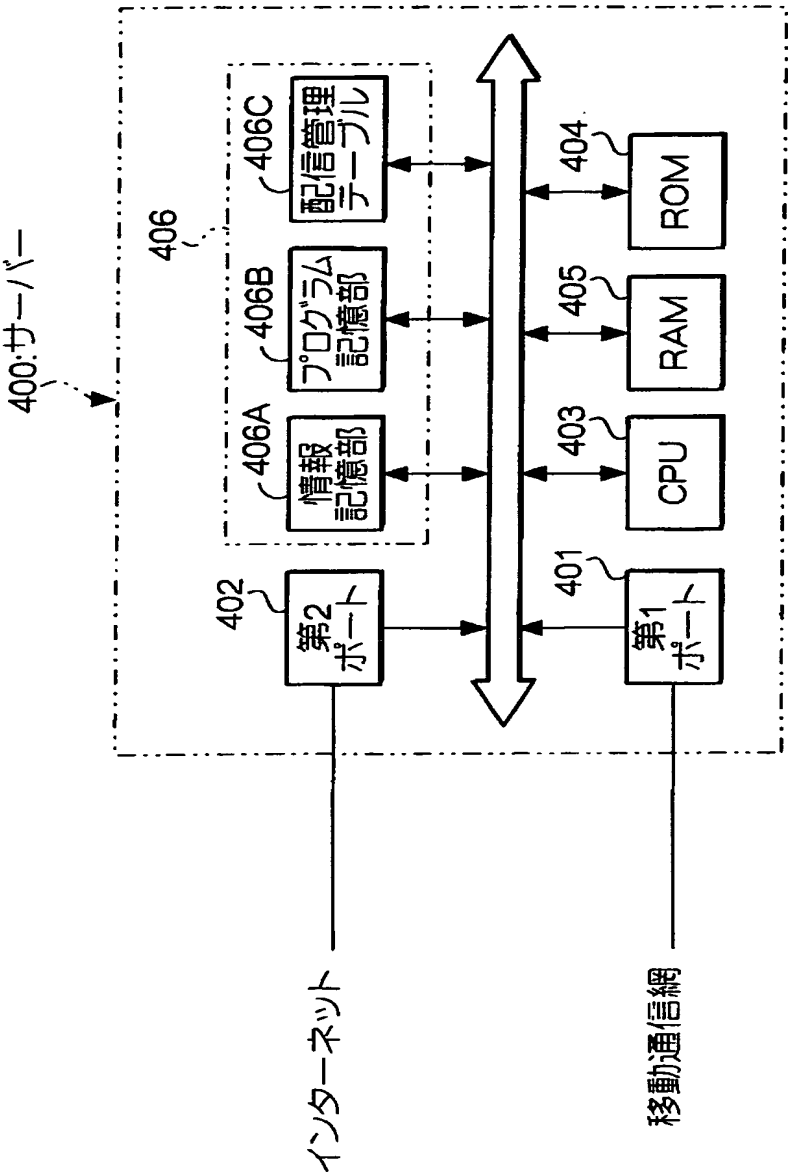
【図２】



【図３】


移動通信網
固定通信網
50:PCカード
11:パソコン
アンテナ
54
通信用送受信部
53
ID記憶部
51B
51
51A
メモリ
コネクタ
55
コントローラ
52
コネクタ
19
モデム
18
表示部
17
キー入力部
16
HDD
15
ROM
13
RAM
14
CPU
12

【図４】


400:サーバー
406
406A
情報記憶部
406B
プログラム記憶部
406C
配信管理テーブル
402
第2ポート
401
第1ポート
403
CPU
405
RAM
404
ROM
インターネット
移動通信網

【図５】

(a)

15A

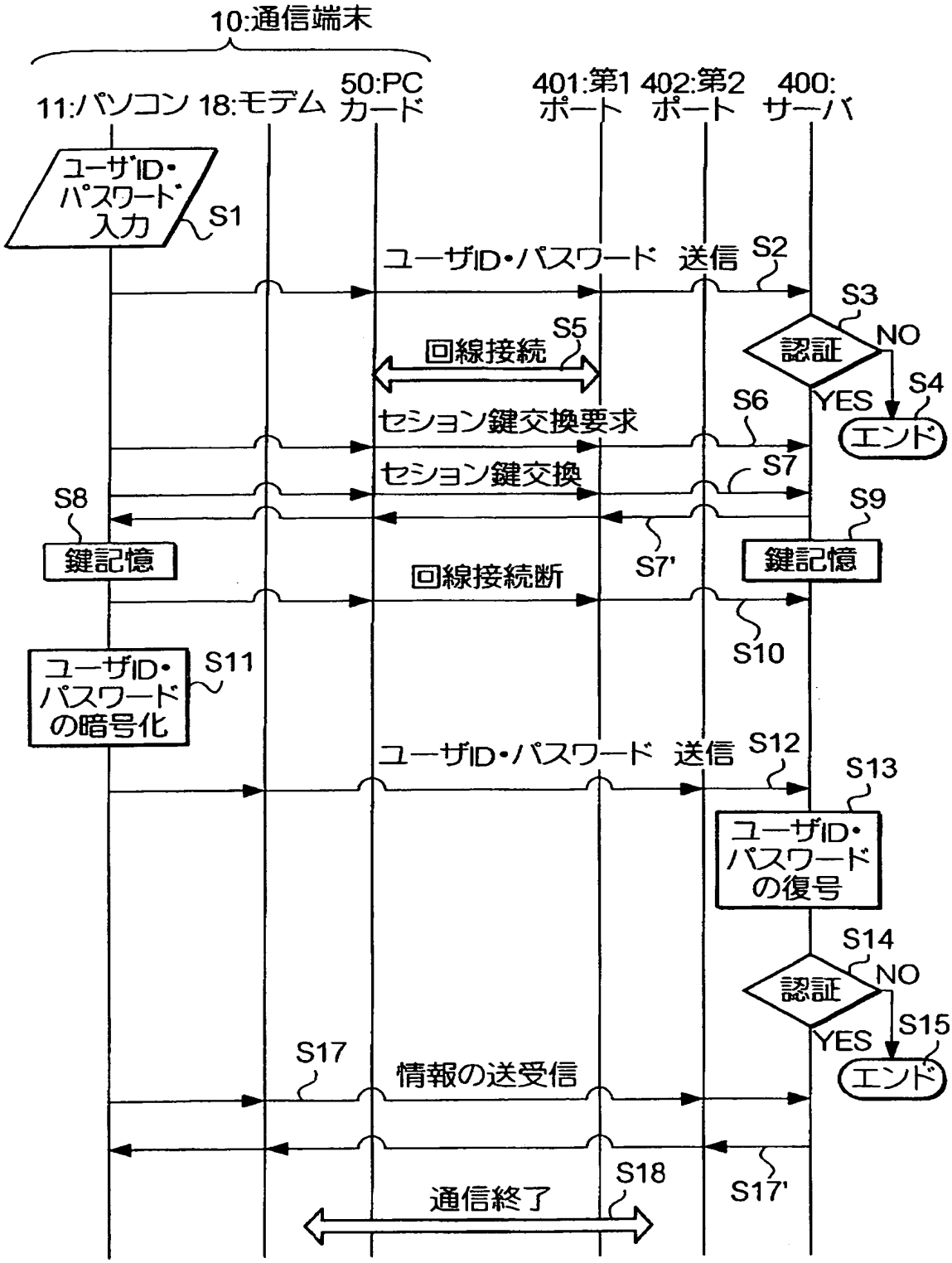
公開鍵 （セッション鍵）	秘密鍵
POkey1	PSkey1
POkey2	PSkey2
⋮	⋮
POkeyn	PSkeyn

(b)

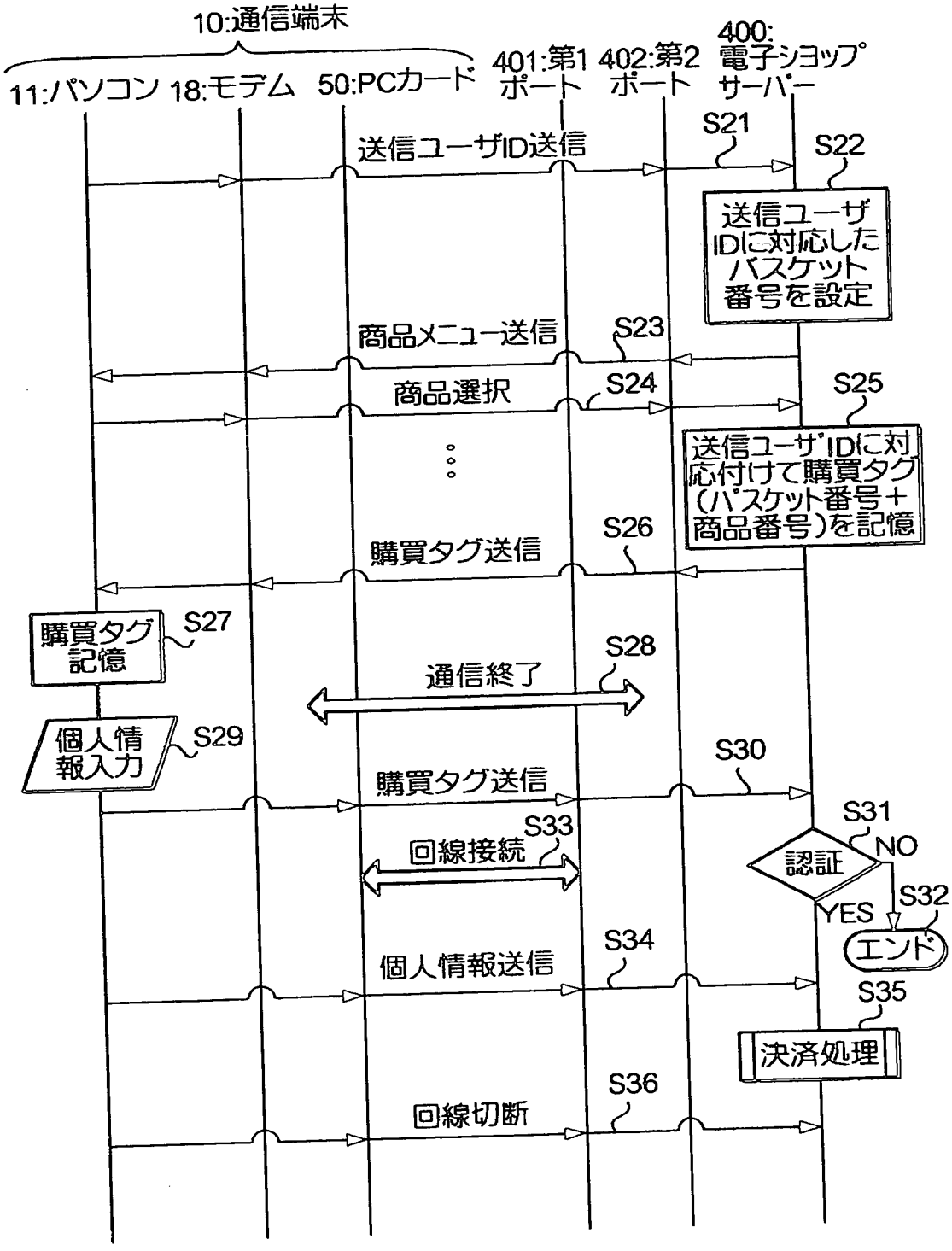
406D

公開鍵 （セッション鍵）	秘密鍵
SOkey1	SSkey1
SOkey2	SSkey2
⋮	⋮
SOkeyn	SSkeyn

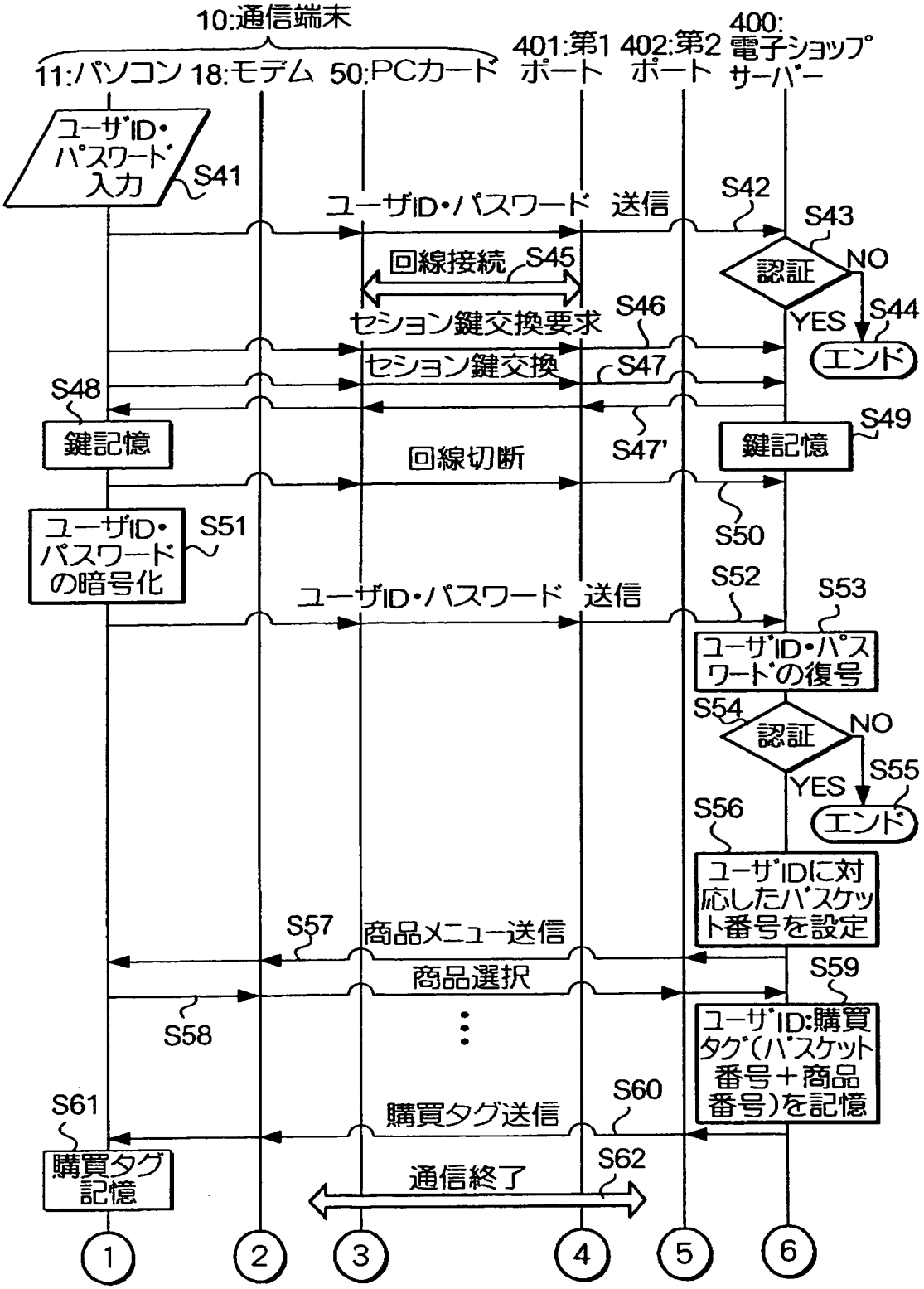
【図６】


10:通信端末
11:パソコン
18:モデム
50:PCカード
401:第1ポート
402:第2ポート
400:サーバ
ユーザID・パスワード入力
S1
ユーザID・パスワード 送信
S2
S3
認証
NO
YES
S4
エンド
回線接続
S5
セション鍵交換要求
S6
セション鍵交換
S7
S7'
S8
鍵記憶
S9
鍵記憶
回線接続断
S10
ユーザID・パスワードの暗号化
S11
ユーザID・パスワード 送信
S12
S13
ユーザID・パスワードの復号
S14
認証
NO
YES
S15
エンド
S17
情報の送受信
S17'
S18
通信終了

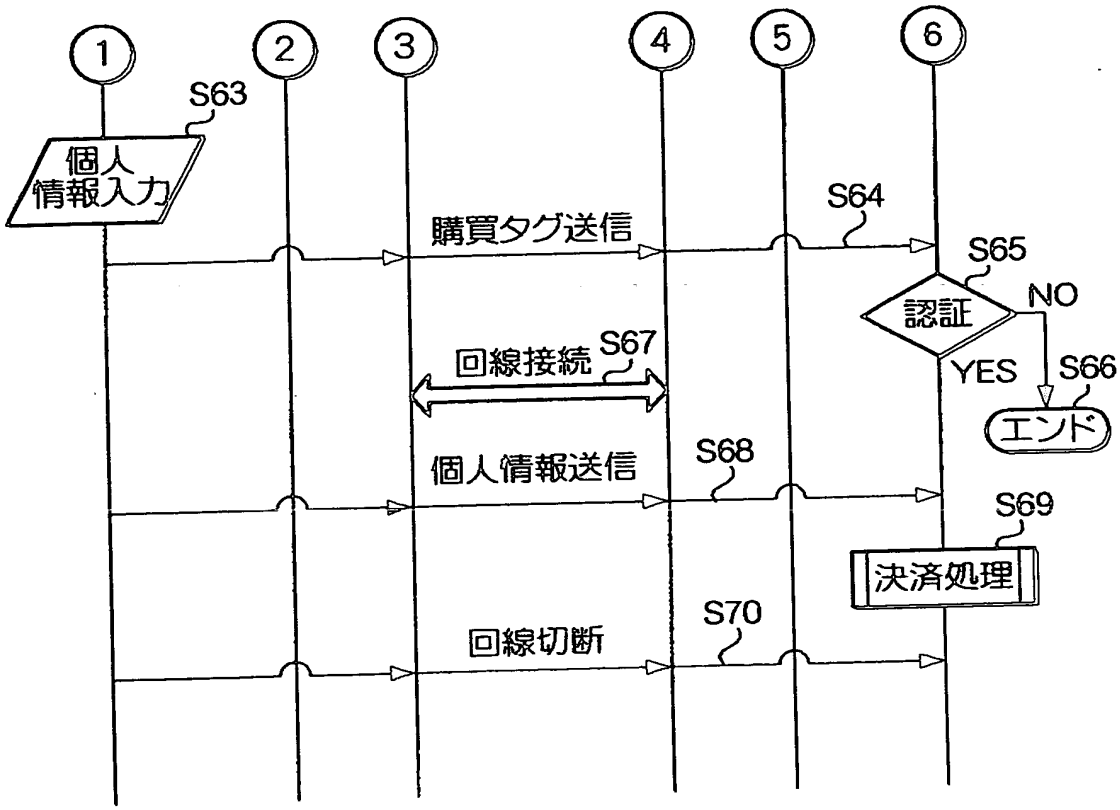
【図７】


10:通信端末
11:パソコン
18:モデム
50:PCカード
401:第1ポート
402:第2ポート
400:電子ショップサーバー
送信ユーザID送信
S21
S22
送信ユーザIDに対応したバスケット番号を設定
商品メニュー送信
S23
商品選択
S24
S25
送信ユーザIDに対応付けて購買タグ(バスケット番号＋商品番号)を記憶
購買タグ送信
S26
購買タグ記憶
S27
通信終了
S28
個人情報入力
S29
購買タグ送信
S30
回線接続
S33
S31
認証
NO
YES
S32
エンド
個人情報送信
S34
S35
決済処理
回線切断
S36

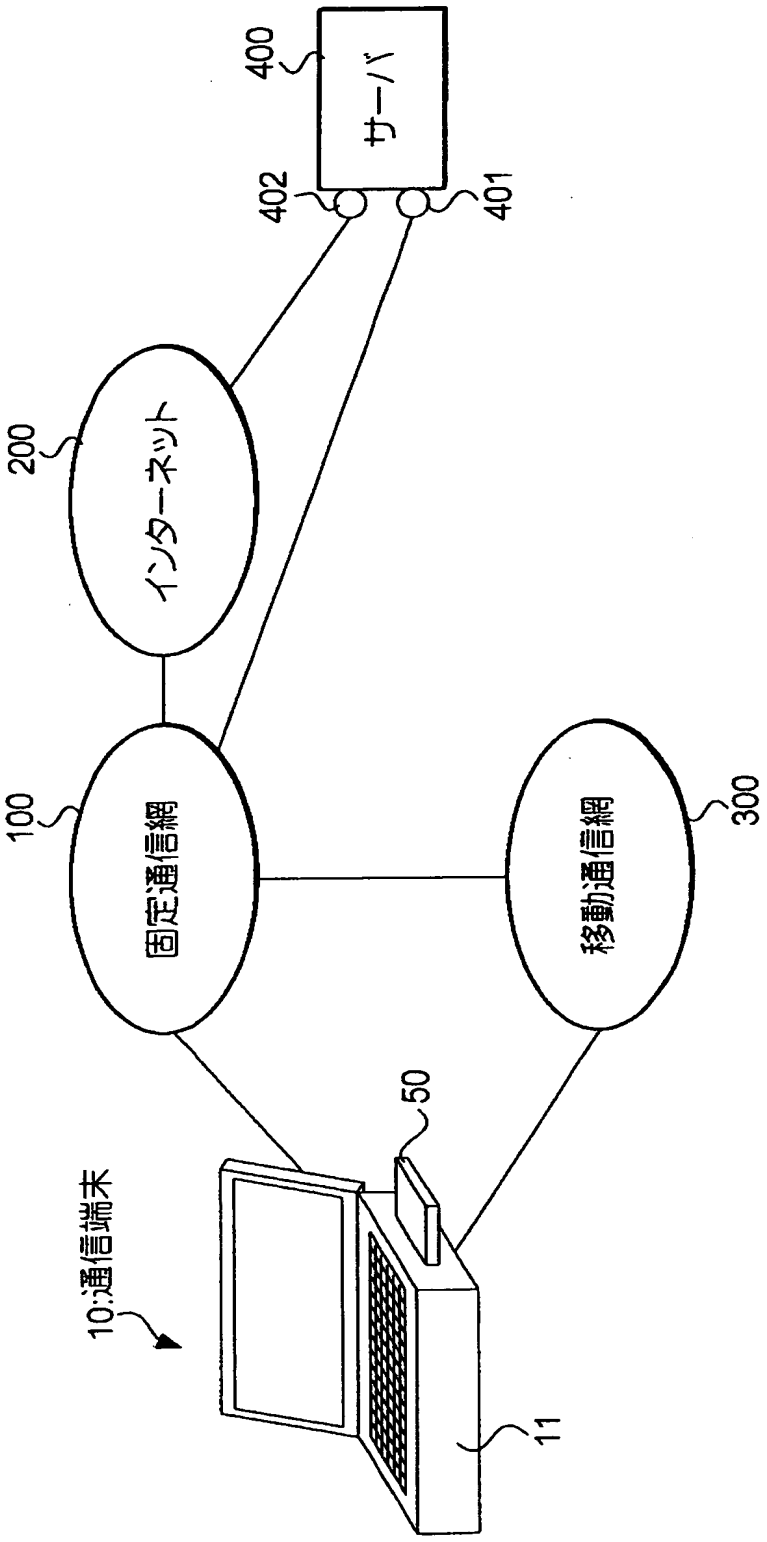
【図８】


10:通信端末
11:パソコン
18:モデム
50:PCカード
401:第1ポート
402:第2ポート
400:電子ショップサーバー
ユーザID・パスワード入力
S41
ユーザID・パスワード 送信
S42
S43
認証
NO
YES
S44
エンド
回線接続
S45
セション鍵交換要求
S46
セション鍵交換
S47
S47'
S48
鍵記憶
S49
鍵記憶
回線切断
S50
ユーザID・パスワードの暗号化
S51
ユーザID・パスワード 送信
S52
S53
ユーザID・パスワードの復号
S54
認証
NO
YES
S55
エンド
S56
ユーザIDに対応したバスケット番号を設定
S57
商品メニュー送信
商品選択
S58
S59
ユーザID:購買タグ(バスケット番号＋商品番号)を記憶
S60
購買タグ送信
S61
購買タグ記憶
通信終了
S62
1
2
3
4
5
6

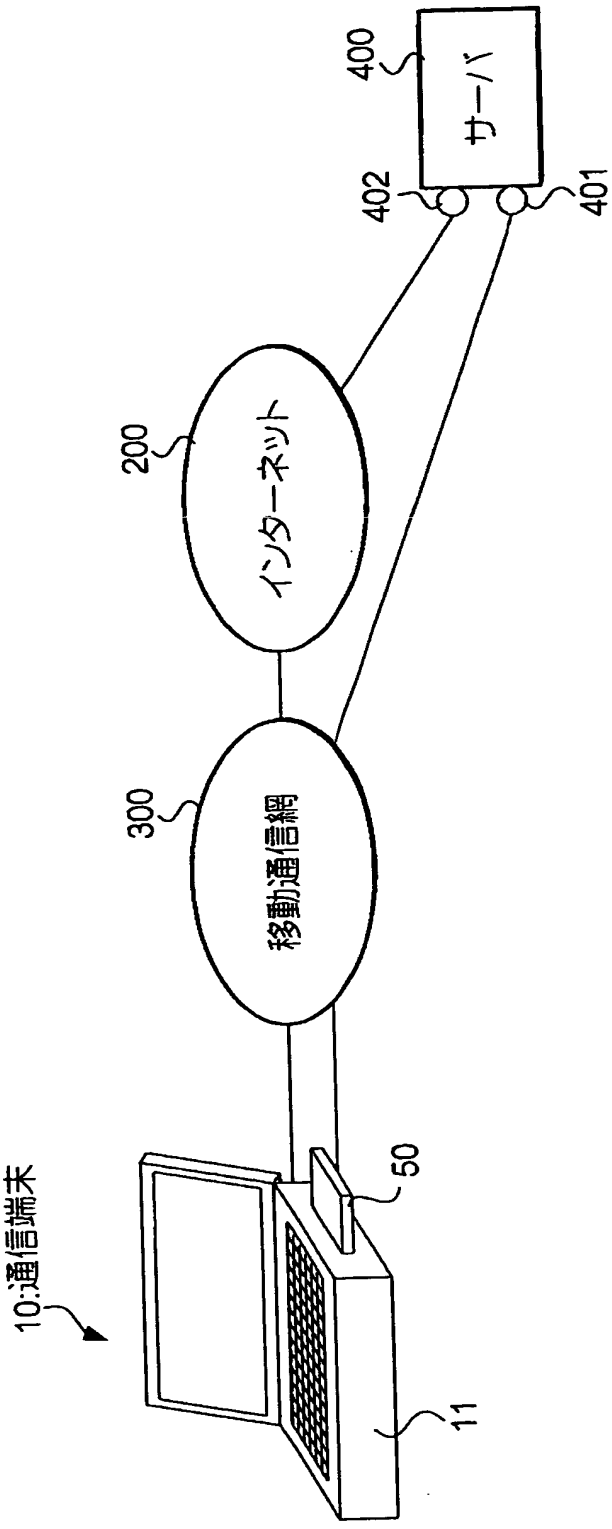
【図９】


1
2
3
4
5
6
S63
個人情報入力
購買タグ送信
S64
S65
認証
NO
YES
S66
エンド
回線接続
S67
個人情報送信
S68
S69
決済処理
回線切断
S70

【図１０】



【図１１】



【書類名】　　要約書

【要約】

【課題】　秘匿を必要とする情報の通信を高いセキュリティを維持し、かつ、迅速に行う秘匿を必要とする。

【解決手段】　通信端末１０は、パソコン１１にＰＣカード５０が装着され、パソコン１１はモデムを介して固定通信網１００に接続され、ＰＣカード５０は移動通信網３００に接続される。サーバ４００の第１ポート４０１は移動通信網３００に接続され、第２ポート４０２はインターネット２００に接続される。秘匿を必要としない情報は、固定通信網１００およびインターネット２００を介して通信を行い、秘匿を必要とする情報は、移動通信網２００を介した回線で行う。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－１５１８７９
受付番号	５００００６３４９１１
書類名	特許願
担当官	佐藤　一博　　１９０９
作成日	平成１２年　５月３０日

＜認定情報・付加情報＞

〔特許出願人〕

〔識別番号〕	392026693
〔住所又は居所〕	東京都千代田区永田町二丁目１１番１号
〔氏名又は名称〕	株式会社エヌ・ティ・ティ・ドコモ

〔代理人〕　申請人

〔識別番号〕	100098084
〔住所又は居所〕	東京都中央区日本橋三丁目２番１６号　八重洲マスヤビル５階　朝日特許事務所
〔氏名又は名称〕	川△崎▽　研二

〔選任した代理人〕

〔識別番号〕	100111763
〔住所又は居所〕	東京都中央区日本橋３丁目２番１６号　八重洲マスヤビル５階　朝日特許事務所
〔氏名又は名称〕	松本　隆

〔選任した代理人〕

〔識別番号〕	100108936
〔住所又は居所〕	東京都中央区日本橋３丁目２番１６号　八重洲マスヤビル５階　朝日特許事務所
〔氏名又は名称〕	秦　貴清

次頁無

出 願 人 履 歴 情 報

識別番号　〔３９２０２６６９３〕

１．変更年月日　２０００年　５月１９日
［変更理由］　名称変更
住　所　東京都千代田区永田町二丁目１１番１号
氏　名　株式会社エヌ・ティ・ティ・ドコモ